Titulo de la Tesis:

"SOBRE RAÍCES PRIMITIVAS"

TESIS

Sometida para optar al título de Maestría en Matemática

Vicerrectoría de Investigación y Postgrado

Facultad de Ciencias Naturales, Exactas y Tecnología

APROBADO POR:

Doctor Jaime Gutiérrez
Presidente

Doctor Julio Vallarino
Miembro

Profesor Narciso Rodríguez
Miembro

REFRENDADO POR:

REPRESENTANTE DE LA VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

FECHA: 16/09/2016.

UNIVERSIDAD DE PANAMÁ

VICERRECTORÁ DE INVESTIGACIÓN Y POSTGRADO

FACULTAD DE CIENCIAS NATUTALES, EXACTAS Y TECNOLOGÍA

PROGRAMA DE MAESTRÍA

SOBRE RAÍCES PRIMITIVAS

GUADALUPE Y. VELÁSQUEZ B.

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OPTAR AL GRADO DE MAGISTER EN CIENCIAS CON ESPECIALIZACIÓN EN MATEMÁTICA PURA

PANAMÁ REPÚBLICA DE PANAMÁ

2016

AGRADECIMIENTO

Doy gracias en primer lugar a Dios todopoderoso por darme la fortaleza y la fe para culminar este trabajo y alcanzar otra meta.

Agradezco al Dr. Jaime Gutiérrez por su valiosa asesoría en el desarrollo del mismo.

Igualmente quiero agradecerle al Dr. Josué Ortiz por sus atinados consejos y oportuna orientación y a todas las personas que de una manera u otra colaboraron con la culminación de este trabajo.

DEDICATORIA

A mis padres Miguel Ángel Velásquez Morales (q.e.d.p.) y Guadalupe Briones de Velásquez quienes lucharon por mi bienestar, mi educación, mi salud y me impulsan siempre a trazar nuevas metas y alcanzar mis objetivos.

También dedico este esfuerzo a mis hermanos Yuly, Quibián y Nika; sobrinos, Solange, Peter, Thiago y Diego quienes me brindan su apoyo y comparten mis triunfos.

Dedicado también a mis familiares y amigos que me apoyaron siempre.

Lupita.

RESUMEN

Se presenta un estudio sobre la construcción de raíces primitivas de un entero dado en términos de una de ellas, por un lado. En contraste con esto se da una construcción explícita de todas las raíces primitivas de p^2 a partir de las raíces de p, donde p es cualquier primo impar. Finalmente se muestra como construir las raíces primitivas de p^{k+1} a partir de las raíces primitivas de p^k, con p un primo impar y $k \geq 2$. Este método permite construir las raíces primitivas de una potencia arbitraria de un número primo en términos de las raíces primitivas de los números primos.

SUMMARY

It is presented the construction of the primitive roots of an integer in terms of one of them. In contrast, we study an explicit construction of all the primitive roosts of p^2 from the primitive roots of p, where p is any prime. Finally, it is shown a method for the construction of the primitive roots of p^{k+1} from those of p^k, where $k>2$, and p is an odd prime. This construction yields all primitive roosts of an arbitrary prime power in terms of the primitive roots of the primes.

Introducción

En los cursos de algebra abstracta de nivel de Licenciatura en Matemática, se estudia entre otros temas el pequeño Teorema de Fermat, que establece la existencia de soluciones para la congruencia $a^x \equiv 1\ mod\ (p)$ con a y p relativamente primos. También forma parte de dicho curriculum la función de Euler. Estos dos tópicos se relacionan de una manera especial para definir el concepto de raíz primitiva de un número entero.

En la presente investigación bibliográfica se busca probar en primer lugar la existencia de raíces primitivas y sus propiedades más relevantes.

El trabajo lo hemos estructurado en tres capítulos. En el primero hacemos una breve reseña histórica de la Teoría de los números, así como una introducción a la aritmética modular resaltando las propiedades más importantes de la función φ de Euler y los sistemas residuales reducidos y completos.

En el segundo capítulo se define las congruencias polinomiales, el orden de un entero positivo módulo un primo p dado, se introduce el concepto de raíz primitiva y se caracterizan los enteros que poseen raíces primitivas, lo cual prueba la existencia de raíces primitivas. Se concluye el capítulo con los Teoremas fundamentales relacionados a las raíces primitivas y el Lema de Hensel mismos.

En el tercer capítulo se presentan los teoremas claves de la investigación. Especial énfasis se hace en la derivación de raíces primitivas a partir de raíces conocidas. Por ejemplo se hace la construcción explícita de las raíces primitivas de p^2 a partir de las de p, siendo p cualquier primo impar.

Finalmente, se presentan el Teorema de Nieven y el caso especial de la construcción de raíces primitivas para potencias arbitrarias de un primo impar, lo cual constituye el resultado principal de la investigación.

INDICE

I. ARITMETICA MODULAR

I. Aritmética Modular

1.1 Reseña Histórica

La Teoría de los números ocupa un lugar especial en la historia de la Matemática, y a través de los siglos puede notarse un interés continuo, tanto de matemáticos como de entusiastas de la Matemática, por las relaciones y propiedades numéricas desde los pitagóricos hasta nuestros días. En primer lugar se mostró interés por clasificar y caracterizar los números primos y compuestos y las correspondientes propiedades de la divisibilidad.

Por otro lado, los números perfectos han captado la atención de los matemáticos de todos los siglos de la era cristiana.

Recordemos que un número es perfecto si es igual a, la suma de sus divisores exceptuándolo a él mismo.

Euclides probó que $2^{p-1}(2^p - 1)$ es un número perfecto siempre que $2^p - 1$ sea primo. Por ejemplo, para p = 2, 3, 5,7; la expresión $2^p - 1$ produce los valores 3, 7, 31 y 127 los cuales son primos; de donde 6, 28, 496 y 8128 son números perfectos de acuerdo a la fórmula de Euclides.

En 1456, se observó que para p =13 se obtiene el número 33550336 que es el quinto número perfecto.

En general los matemáticos se esforzaron por encontrar una regla que permitiera caracterizar todos los números perfectos, aplicando alguna propiedad de los números primos.

Por ejemplo $\mathbf{Z}_7$, consta de las siguientes clases de equivalencia

$$[0] = \{x \in \mathbf{Z}, x = 7t, t \in \mathbf{Z}\}$$

$[1] = \{x \in \mathbf{Z}, x = 7t+1, t \in \mathbf{Z}\}$

$[2] = \{x \in \mathbf{Z}, x = 7t+2, t \in \mathbf{Z}\}$

$[3] = \{x \in \mathbf{Z}, x = 7t+3, t \in \mathbf{Z}\}$

$[4] = \{x \in \mathbf{Z}, x = 7t+4, t \in \mathbf{Z}\}$

$[5] = \{x \in \mathbf{Z}, x = 7t+5, t \in \mathbf{Z}\}$

$[6] = \{x \in \mathbf{Z}, x = 7t+6, t \in \mathbf{Z}\}$

Teorema 1.2

Para un entero positivo fijo, p son válidas las afirmaciones siguientes:

a. Si $a = qp + r$ entonces $a \equiv r \bmod (p)$

b. Si $0 \leq r' < r < p$ entonces $r \not\equiv r' \bmod (p)$

c. $a \equiv b \bmod (p)$ si y solo si los residuos que resultan al dividir a y b por p son iguales.

Corolario 1.1:

Si $p \geq 2$ entonces todo entero positivo a es congruente mod(p) solo con uno de los elementos del conjunto$\{0,1,\ldots, p-1\}$.

Teorema 1.3

Si se tiene que $a \equiv e$ mod (p) y $b \equiv f$ mod(p) entonces

a. $a + b \equiv e + f$ mod(p)

b. $a - b \equiv e - f \, mod \, (p)$

c. $ab \equiv ef$ mod (p)

d. $ka \equiv ke$ mod (p) donde k es cualquier número entero

e. Si $a \equiv b$ mod (p) entonces $a^n \equiv b^n$ mod p , para todo n en $\mathbb{N}$.

Observaciones:

Sea p un número primo, $\mathbf{Z_p} = {}^{Z}/_{pZ}$ es conjunto finito de p elementos o clases de congruencias. Definamos las operaciones de adición y multiplicación de clases mediante las igualdades siguientes:

$[x] \oplus [y] = [x + y]$, $[x] \odot [y] = [x \cdot y]$. Estas operaciones están bien definidas. Esto es: $\oplus$ y $\odot$ no dependen del representante de la clase de congruencia que se escoja.

Se puede verificar que todas las propiedades de un anillo se cumplen en $\mathbf{Z}_p$, respecto a las operaciones de adición y multiplicación consideradas anteriormente.

Teorema 1.4

$[a] \in \mathbf{Z}_p$, es *invertible* en $\mathbf{Z}_p$ si a y p son primos *relativos.*

Teorema 1.5

Si p es un entero positivo, entonces $\mathbf{Z}_p$, es un *cuerpo* si y solo si p es primo.

Teorema 1. 6

Si p es un número primo entonces $(a + b)^p \equiv a^p + b^p \bmod (p)$

Teorema 1. 7

(a) Si p es un primo entonces $a^p \equiv a \bmod (p)$, para todo $a \in \mathbf{Z}$.

(b) $a^{p^i} \equiv a \bmod (p)$, para todo $i \geq 1$.

Proposición 1.2

Sean a y b enteros y sea (a,b) = d el máximo común divisor de a y b entonces $\left(\frac{a}{d}, \frac{b}{d}\right)=1$

Lema

Si a, b y c son enteros positivos tales que (a,b)=1 si a/bc necesariamente a/c.

1.3 Clases residuales y aritmética (mod p).

. **Definición 1.1** (Sistema Residual completo)

Los números enteros $a_1, a_2, \ldots, a_p$, que constituyen un sistema residual completo módulo m están caracterizado por las siguientes propiedades:

a) Si $i \neq j$, entonces $a_i \not\equiv a_j \pmod{p}$.

b) Si a es cualquier entero, existe un único índice i con $1 \leq i \leq p$ para el cual

$a \equiv a_i \pmod{p}$.

El conjunto de enteros 0, 1, 2,. . . . , p – 1 y el conjunto 1, 2,..., p, son ejemplos de sistemas residuales completos (mod p). Los elementos de un sistema residual completo no necesitan ser enteros consecutivos; por ejemplo, para p = 5 podríamos tomar 1, 22, 13, - 6,2500.

En general, si escribimos las cinco progresiones aritméticas son

diferencia 5:

. . ., -10, -5, 0, 5, 10, 15,. . .,

. . ., -9, -4, 1, 6, 11, 16,. . .,

. . ., -8, -3, 2, 7, 12, 17,. . .,

. . ., -7, -2, 3, 8, 13, 18,. . .,

. . ., -6, -1, 4, 9, 14, 19,. . .,

Podríamos escoger cualquier elemento de cada renglón; el de la primera línea es representativo de todos los enteros divisibles por 5, el del segundo es representativo de todos los enteros de la forma 5n + 1, el de la tercera línea es representativo de los todos los enteros de la forma 5n + 2, etc.

Teorema 1.8

Si $a_1, a_2, \ldots, a_p$ es un sistema residual completo (mod p) y $(k, p) = 1$, entonces ka_1, $ka_2, \ldots, ka_p$ es también un sistema residual completo (mod p).

1.4 Sistemas residuales y la función φ de Euler.

La razón de que usamos el adjetivo "completo" cuando hablamos de un sistema residual es que existe otra clase que también es usada con frecuencia, llamado sistema residual reducido. Este es un conjunto de enteros $a_1, \ldots, a_h$ incongruentes (mod p) y primos relativos con p, tales que si a es cualquier entero elativamente primo con p, existe un índice i, $1 \leq i \leq h$, para el cual $a \equiv a_i \pmod{p}$. En otras palabras, un sistema residual reducido es un conjunto de representativos, uno por cada una de las clases residuales, que contiene enteros primos relativos con p.

Definición 1.2

El número h de elementos en un sistema residual reducido (mod p) es el número de enteros positivos menores que p y primos con p. Este número h que depende de p, es

designada por costumbre como φ(p) y define la función φ de Euler (en honor al matemático suizo Leonard Euler).

La tabla siguiente muestra los primeros 30 valores de la función de Euler.

p	ϕ (p)	p	ϕ (p)	p	ϕ (mp)
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Tabla 1

Teorema 1.9

Si $a_1, \ldots, a_{\varphi(p)}$ es un sistema residual reducido (mod p) y (k, p) = 1, entonces también $ka_1, \ldots, ka_{\varphi(p)}$ es un sistema residual reducido (mod p).

1.5 Propiedades de la función de Euler

1. Si $p > 2$ entonces $\varphi(p)$ es par. Consideremos el conjunto A_p definido por $A_p = \{a \in \bar{Z}^+ / a < p \text{ y } (p,a) = 1\}$ es claro que $\varphi(p)$ es el cardinal de A_p por definición. Por otro lado, si escogemos un elemento a en A_p, podemos ver $p - a$ también pertenece a A_p, ya que $0 < p - a < p$ y además como $1 = (a, p) = (p - a, p)$. Lo anterior muestra que los elementos de A_p pueden agruparse de dos en dos, por lo cual su cardinal es un entero positivo par.
2. Si p es un número primo entonces $\varphi(p) = p - 1$.
3. Los valores de la función φ parecen ser bastante irregulares. Sin embargo es posible calcular rápidamente el valor de $\varphi(p)$ si es conocida la factorización de p en primos. Un hecho que se observa de la tabla 1, es que en ciertos casos los valores de $\varphi(p)$ y $\varphi(n)$ pueden ser multiplicados para obtener $\varphi(pn)$; por ejemplo, $\varphi(3)\,\varphi(7) = \varphi(21)$ y $\varphi(4)\,\varphi(5) = \varphi(20)$. Por otro lado, $\varphi(4)\,\varphi(6) \neq \varphi(24)$. El resultado preciso lo presentamos en el teorema siguiente.

Teorema 1.10

Si $(p,n) = 1$, *entonces* $\varphi(pn) = \varphi(p)\,\varphi(n)$

(Una función que satisface esta propiedad se llama función multiplicativa)

Prueba:

Consideremos los enteros p,n con (p, n) =1 y los números de la forma $px + ny$. Si podemos restringir los valores de x y y, suponiendo que estos números forman un sistema residual reducido (mod pn), la cantidad de ellos debe ser φ (pn). Pero su número es también el producto del número de valores que pueda tomar x por el número de valores que pueda tomar y. Claramente, para que $px + ny$ sea primo a m, es necesario que $(p, y) = 1$ y también que $(n, x) = 1$. Inversamente, si se satisfacen estas dos últimas condiciones, entonces

$(px + ny, pn) = 1$, puesto que en este caso cualquier primo divisor de p o de n, divide exactamente uno de los dos términos en $px + ny$. Por lo tanto, considérese que x toma valores en un sistema residual reducido (mod n), digamos $x_1,\ldots x_{\varphi(n)}$ y que y toma valores en un sistema residual reducido (mod m), digamos $y_1,\ldots., y_{\varphi(p)}$. Si para algunos índices i, j, k, l tenemos

$$px_l + ny_j \equiv px_k + ny_l \pmod{pn},$$

entonces

$$p(x_l - x_k) + n(y_j - y_l) \equiv 0 \pmod{pn}$$

Como la divisibilidad por pn implica divisibilidad por p, tenemos

$$p(x_i - x_k) + n(y_j - y_l) \equiv 0 \pmod{p},$$

$$n(y_j - y_l) \equiv 0 \pmod{p},$$

$$y_j \equiv y_l \pmod{p}$$

por lo que j = 1. En forma similar, i = k. De esta manera los números $px + ny$ así formados, son incongruentes (mod pn). Considérese ahora que a es cualquier entero primo con pn, en particular

(a,p)=1 y (a, n)=1. Entonces se demuestra que existen X, Y enteros (no necesariamente en los sistemas residuales reducidos escogidos), tales que $pX + nY = a$, por lo que también $pX + nY \equiv a \pmod{pn}$, Como $(p, Y) = (n, X) = 1$, existe una x_i tal que $X \equiv x_i \pmod{n}$ y una y_j tal que $Y \equiv y_j \pmod{p}$. Esto significa que existen k, l enteros tales que

$X = x_i + kn$, $Y = y_j + lp$. Por lo tanto,

$pX + nY = p(x_i + kn) + n(y_j + lp) \equiv px_i + ny_j \equiv a \pmod{pn}$.

De aquí, como x y y toman valores en los sistemas residuales reducidos (mod n) y (mod p), respectivamente, $px + ny$ toma valores sobre un sistema residual reducido (mod pn), con lo cual se completa la demostración.

Teorema 1.11

Sea n un entero positivo. Entonces $\sum_{d/n} \varphi(d) = n$

Prueba:

Descomponemos los enteros desde 1 hasta n en clases, de la manera siguiente localizamos el entero m en la clase C_d si el máximo común divisor de m y n es d. Observemos que m pertenece a C_d, esto es: (m,n) = d si y sólo si $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Así pues, la cantidad de enteros pertenecientes a C_d es el número de enteros positivos no mayores que $\frac{n}{d}$ y que son relativamente primos con $\frac{n}{d}$. De esta observaión se ve que hay $\varphi(\frac{n}{d})$ enteros en C_d. Como hemos dividido los enteros desde 1 hasta n en clases desjuntas y cada entero pertenece exactamente a una sola de ellas, n es la suma de las cantidades de elementos de las diferentes clases.

Consecuentemente, se aprecia que $n = \sum_{d/n} \varphi\left(\frac{n}{d}\right)$

Así pues $n = \sum_{d/n} \varphi\left(\frac{n}{d}\right) = \sum_{\frac{n}{d}} \varphi(d)$, lo que finaliza la prueba.

II. CONGRUENCIAS POLINOMIALES Y RAÍCES PRIMITIVAS

II. Congruencias Polinomiales.

En esta sección nos proponemos determinar aquellos números enteros que tienen raíces primitivas. Se mostrara que todo número primo tiene una raíz primitiva, para lo cual se necesita el estudio de la congruencia polinomial.

Definición 2.1

Sea $f\ (x)$ un polinomio con coeficientes enteros, diremos que un entero c es una raíz de $f(x)$ módulo m si $f\ (c)\ \equiv\ 0\ mod\ (m)$.

Observación: es fácil ver que si c es una raíz de $f\ (x)$ módulo m, entonces todo entero congruente con $c\ mod\ (m)$ es también una raíz de $f\ (x\ )\ mod\ (m)$.

Ejemplos:

a) El polinomio $f(x)\ =\ x^2\ +\ x\ +\ 1$ tiene exactamente dos raíces no congruentes módulo 7, a saber $x\ =\ 2$ y $x\ =\ 4$.

b) El polinomio $f(x)\ =\ x^2\ +\ 2$ no tiene raíces módulo 5.

c) Si p es un entero primo, por el pequeño teorema de Fermat, el polinomio $f(x)\ =x^{p-1}-\ 1$ tiene exactamente $p-1$ raíces no congruentes $mod(p)$, a saber

$$x\ =\ 1,2,3,\ldots,p-1.$$

Teorema 2.1 (Teorema de Lagrange)

Sea $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_n + a_0$ polinomio de grado n con coeficientes enteros y coeficiente principal a_n no divisible por p. Entonces $f(x)$ tiene a lo sumo n raíces no congruentes módulo p.

Prueba:

La prueba se hará por inducción matemática sobre el grado n del polinomio $f(x)$. Si $n = 1$, tenemos $f(x) = a_1 x + a_0$ con a_1 no divisible por p. Una raíz de $f(x)$ módulo p es una solución de la congruencia lineal

$a_1 x \equiv -a_0 \, mod(p)$. Como a_1 y p son relativamente primos, la congruencia lineal anterior tiene una sola solución la cual es una raíz de $f(x)$ módulo p. Así pues, el teorema es verdadero para $n = 1$.

Supongamos que el teorema es verdadero para polinomios de grado $n - 1$ y sea $f(x)$ un polinomio de grado n con coeficiente principal no divisible por p. Asumamos, por reducción al absurdo, que $f(x)$ tiene $n + 1$ raíces no congruentes módulo p, digamos que $c_0, c_1, \ldots c_n$ tales que $f(c_k) \equiv 0 \, mod(p)$, para $k = 0, 1, \ldots, n$.

Bajo las condiciones anteriores tendremos que

$$f(x) - f(c_0) = a_n(x^n - {c_0}^n) + a_{n-1}(x^{n-1} - {c_0}^{n-1}) + \cdots + a_1(x - c_0)$$

$$= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + x{c_0}^{n-1} + {c_0}^n) + a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + x{c_0}^{n-2} + {c_0}^{n-1}) + \cdots + a_1(x - c_0) = (x - c_0)g(x).$$

donde $g(x)$ es un polinomio de grado $n-1$ y coeficiente principal a_n. Ahora verificaremos que $c_1, c_2, \ldots, c_n$ son todas las raíces de $g(x)\ mod(p)$. Sea k un entero, $1 \leq k \leq n$.

Por cuanto $f(c_k) \equiv f(c_0) \equiv 0\ mod(p)$ se tiene que

$$f(c_k) - f(c_0) = 0g(c_k) \equiv 0\ mod\ (p).$$

De esto último se concluye que $g(c_k) \equiv 0\ mod\ (p)$ ya que $c_k - c_0 \not\equiv$ o mod (p). Así pues c_k es una raíz de $g(x)$ módulo p, para todo k tal que $1 \leq k \leq n$. Se ha mostrado que $g(x)$, que tiene grado $n-1$ y coeficiente principal no divisible por p, tiene n raíces no congruentes módulo p. Pero esto contradice la hipótesis inductiva. En conclusión

$f(x)$ no puede tener más de n raíces no congruentes módulo p, lo cual concluye la inducción y el teorema queda probado.

Teorema 2.2

Sea p un entero primo y d un divisor de $p-1$. Entonces el polinomio $x^d - 1$, tiene exactamente d raíces no congruentes módulo p.

Prueba:

Sea $p-1$ entonces,

$$x^{p-1} - 1 = x^{de} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \ldots + 1) = (x^d - 1)\, g(x)$$

Por el pequeño teorema de Fermat, se observa que $x^{p-1} - 1$ tiene $p - 1$ raíces no congruentes módulo p.

Más aun, cualquier raíz de $x^{p-1} - 1$ módulo p es ó bien una raíz de $x^d - 1$ ó una raíz de $g\ (x)$ módulo p.

Por el teorema de Lagrange, Teorema 2.1, $g\ (x)$ tiene a lo sumo

$d(e - 1) = p - d - 1$ raíces módulo p. Como cada raíz de $x^{p-1} - 1$ módulo p que no sea una raíz módulo p de $g\ (x)$ debe ser una raíz de $x^d - 1$ módulo p, se infiere que el polinomio $x^d - 1$ tiene por lo menos $(p - 1) - (p - d - 1) = d$ raíces no congruentes módulo p. Por otro lado, el teorema de Lagrange nos dice que $x^d - 1$ tiene a lo sumo d raíces no congruentes módulo p

Consecuentemente, $x^d - 1$ tiene exactamente d raíces no congruentes módulo p.

A continuación veremos cómo se aplica el teorema anterior para determinar cuántos enteros no congruentes tienen un mismo orden módulo p.

Sea φ la función de Euler, si m es un entero positivo y a es un entero relativamente primo con m, entonces $a^{\varphi(m)} \equiv 1\ mod(m)$. Por lo tanto, existe al menos un entero positivo x que satisface la congruencia $a^x \equiv 1\ mod(m)$. En consecuencia, por el principio del buen orden, existe un menor entero positivo x que satisface dicha congruencia. Esto último motiva la siguiente definición.

Definición 2.2

Sean a y m enteros positivos relativamente primos. Entonces, al menor entero positivo x tal que

$a^x \equiv 1\ mod(m)$ se le llama orden de a módulo m y lo denotamos $ord_m a$.

Ejemplos

Para encontrar el orden de 2 $módulo$ 7, computamos sucesivamente las potencias

$2^1 = 2 \equiv 2\ mod(7)$, $2^2 = 4 \equiv 4\ mod(7)$, $2^3 = 8 \equiv 1\ mod(7)$ de donde se concluye que $ord_7 2 = 3$

Similarmente los cálculos $4^1 = 4 \equiv 4\ mod(7)$, $4^2 = 16 \equiv 2\ mod(7)$, $4^3 = 64 \equiv 1\ mod(7)$ de donde se concluye que $ord_7 4 = 3$

Análogamente se puede comprobar que $ord_7 5 = 6$

Teorema 2.3

Sea p un número primo y sea d un divisor positivo de $p - 1$. Entonces el número de enteros no congruentes de orden d módulo p es $\varphi(d)$.

Prueba:

Sea p un número primo. Para cada d divisor positivo de $p - 1$, definamos $F(d)$ como el número de enteros positivos menores que p cuyo orden módulo p sea d. Como

el orden módulo p de un número entero no divisible por p divide a $p - 1$, se deduce que:

$$p - 1 = \sum_{d/p=1} F(d)$$

Por el teorema 1.11, se sabe que:

$$p - 1 = \sum_{d/p-1} \varphi(d)$$

A continuación verificamos que si $d / p - 1$ entonces $F(d) \leq \varphi(d)$.

Esta desigualdad conjuntamente con la igualdad $\sum_{d/p-1} F(d) = \sum_{d/p-1} \varphi(d)$

nos conduce a la igualdad $F(d) = \varphi$ (d) para cada divisor positivo d de p – 1.

En efecto, supongamos que d/ p–1. Si F (d) = 0, es claro que $F(d) \leq \varphi(d)$.

Si $F(d) \neq 0$, existe un entero a de orden d módulo p.

Ahora bien, si $ord_p(a) = d$, los enteros $a^1, a^2, \ldots, a^d$, son incongruentes módulo p. Más aún, cada una de estas potencias es una raíz del polinomio $x^d - 1$ módulo p, toda vez que $(a^k)^d \equiv (a)^{dk} \equiv 1 \, mod\,(p)$ para cada entero que $x^d - 1$ tiene exactamente d raíces incongruentes módulo p, así que cada raíz módulo p debe ser congruente con una de estas potencias. Sin embargo, del Teorema 2.3 se sabe que las potencias de a cuyo orden módulo p sea d son aquellas que tienen la forma a^k con $(k, d) = 1$.

Ya se sabe que hay exactamente $\varphi(d)$ enteros k con $1 \leq k \leq d$, que satisfacen esta condición, y consecuentemente, si hay un entero de orden d módulo p, el total de estos es exactamente $\varphi(d)$. De esto último, se concluye que $F(d) \leq \varphi(d)$.

Por lo tanto, concluimos que $F(d) = \varphi(d)$, lo cual significa que hay exactamente

$\varphi(d)$ enteros no congruentes módulo p cuyo orden es d.

Teorema 2.4

Si a y m son enteros relativamente primos entre si y $m > 0$, entones un entero positivo x es una solución de la congruencia $a^x \equiv 1\ mod(m)$ si y solo si $ord_m a/x$.

Prueba:

Supongamos que x es un múltiplo de $ord_m a$, entonces $x = k \cdot ord_m a$ donde k es un entero positivo. En consecuencia, $a^x = a^{k \cdot ord_m(a)} = a^{ord_m(a)^k} \equiv 1\ mod(m)$. Recíprocamente, asumiendo que x es un entero positivo tal que $a^x \equiv 1\ mod(m)$, al realizar la división euclidiana de x por $ord_m a$

Se obtiene lo siguiente: Existen enteros r, q tales que:

(*) x = q· $ord_m a$ + r con $0 \leq r < ord_m a$ de esta ecuación se observa que

$a^x = a^{q \cdot ord_m(a)+r} = a^{ord_m(a)^q} \cdot a^r \equiv a^r\ mod(m)$. Como por hipótesis

$a^x \equiv 1\ mod(m)$ y

$a^x \equiv a^r\ mod(m)$ por transitividad se concluye que $a^r \equiv 1\ mod(m)$. Esto último y la desigualdad $0 \leq r < ord_m a$ se concluye que $r = 0$ por la definición de $ord_m a$ como el menor exponente x tal que $a^x \equiv 1\ mod(m)$. Finalmente de (*) se tiene que

$x = q \cdot ord_m a$, esto es $ord_m a$ /x.

A continuación se presenta una consecuencia inmediata de este teorema.

Corolario 2.1

Si a y m son enteros relativamente primos y $m > 0$, entones $ord_m a \,/\varphi(m)$.

Prueba:

Como a y m son enteros relativamente primos por el teorema de Euler

$a^{\varphi(m)} \equiv 1 \, mod(m)$ aplicando el teorema 2.4 se concluye efectivamente que $\varphi(m)$ es un múltiplo de $ord_m a$.

Teorema 2.5

Si a y m son enteros relativamente primos y $m > 0$, entones

$a^i \equiv a^j mod$ (m), donde *i, j* son enteros no negativos, si y solo si $i \equiv j \, mod(ord_m a)$

Prueba:

Supongamos que $i \equiv j \, mod(ord_m a)$. Entonces $i - j = k \, ord_m a$ para algún k en Z^+

y así pues $a^i = a^{j+kord_m(a)}$

$$= a^j \, (a^{ord_m(a)})^k$$

$$\equiv a^j \, mod \, (m) \text{ pues } a^{ord_m(a)} \equiv 1 \, mod \, (m)$$

Recíprocamente, si aceptamos que $a^i \equiv a^j mod \, (m)$ con $i \geq j$, entonces como

$(a, m) = 1$

También $(a^j, m) = 1$.

Ahora bien, $a^i = a^{i+j-j} = a^j a^{i-j} \equiv a^j \, mod\ (m)$ implica que $a^{i-j} \equiv 1 \, mod\ (m)$

De esto último aplicado en teorema 2.4 que $i - j$ debe ser divisible entre $ord_m(a)$

Es decir, $i - j = k \ ord_m(a)$ para algún $k \geq 0$ lo cual significa que

$i \equiv j \, mod\ (ord_m(a))$

A continuación nos fijaremos en aquellos enteros a cuyo orden sea exactamente $\varphi(m)$.

2.2 Raíces Primitivas

Definición 2.3

Si a y m son enteros relativamente primos y m > 0 y si el ord $_m$(a) = $\varphi(m)$ diremos que a es una raíz primitiva módulo m.

Ejemplo:

Sean a = 3, m = 7

Se puede verificar fácilmente ord $_7$(3) = 6. Ya que $\varphi(7) = 6$, se deduce que 3 es una raíz primitiva mod (7). Análogamente, como también el ord $_7$(5) = 6, 5 es raíz primitiva módulo 7.

Observación:

No todos los enteros tienen raíz primitiva. Por ejemplo, no hay raíces primitivas módulo 8. Para verificar esto, observemos que los únicos enteros menores que 8 y relativamente primos con 8 son 1, 3, 5 y 7. Así pues $\varphi(8) = 4$. No obstante,

$\text{ord}_8\, 1 = 1$, $\text{ord}_8(3) = 2$, el $\text{ord}_8(5) = \text{ord}_8(7) = 2$ son distintos de 4.

En lo que sigue de nuestra investigación nos proponemos encontrar todos los enteros que poseen raíces primitivas. El teorema siguiente nos provee una aplicación de las raíces primitivas.

Teorema 2.6

Si a y m son enteros relativamente primos y $m > 0$ y si a es una raíz primitiva módulo m, entonces los enteros $a, a^2, \ldots a^{\varphi(m)}$ forman un sistema residual reducido módulo m.

Prueba

Para demostrar que las primeras $\varphi(m)$ potencias de la raíz primitiva a forman un sistema residual reducido módulo m, basta con mostrar que todas ellas son relativamente primas con m y además no existe un par de ellas que sean congruentes entre si módulo m.

Si $(a,m) = 1$, se concluye que $(a^k, m) = 1$ para todo entero positivo k. Solo resta verificar la segunda parte, esto es: cada potencia define una clase de equivalencia módulo m distinta.

Supongamos lo contrario, esto es: existen potencia a^l, a^j tales que $a^l \equiv a^j \bmod m$

Por el teorema 2.5 se infiere que $i \equiv j \mod (\text{ord}_m a) \equiv j \mod(\varphi(m))$ ya que a es raíz primitiva módulo m. Sin embargo, para $1 \leq i \leq \varphi(m)$ y $1 \leq j \leq \varphi(m)$, la congruencia de $i \equiv j \mod (\varphi(m))$ implica que $i = j$.

En consecuencia, no hay dos potencias de a distintas que sean congruentes módulo m. Esto muestra que $a, a^2, \ldots a^{\varphi(m)}$ es un sistema residual reducido módulo m.

Ejemplo:

2 es una raíz primitiva módulo 9 ya que $2^2 \equiv 4 \mod (9)$; $2^3 = 8 \equiv 8 \mod (9)$;...,

$2^6 \equiv 1 \mod (9)$.

Por el teorema 2.6 las primeras $\varphi(9)$, esto es las primeras 6 potencias de 2 forman un sistema residual reducido módulo 9. En efecto:

$2^1 = 2 \equiv 2 \mod (9)$

$2^2 = 4 \equiv 4 \mod (9)$

$2^3 = 8 \equiv 8 \mod (9)$

$2^4 = 16 \equiv 7 \mod (9)$

$2^5 = 32 \equiv 5 \mod (9)$

$2^6 = 64 \equiv 1 \mod (9)$

Los cálculos anteriores nos muestran que $\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6\}$ es un sistema residual reducido módulo 9.

Veremos a continuación que cuando un entero tiene una raíz primitiva, generalmente tiene muchas raíces primitivas. Para dar una demostración de esto, es necesario el teorema siguiente.

Teorema 2.7:

Si ord $_m$ (a) = t y u es un entero positivo, entonces ord$_m$ (a^u) = $\frac{t}{(t,u)} = \frac{\text{ord}_m(a)}{(t,u)}$

Prueba:

Sean s = ord $_m$ (a^u) y v= (t,u). Entonces t = t_1 v y también u = u_1v para enteros únicos t_1 y u_1. Por la proposición 1.2 se sabe que (t_1 , u_1) = 1.

Observemos que: $(a^u)^t = (a^{u_1 v})^{t/v} = (a^t)^{u_1} \equiv 1 \bmod (m)$

por cuanto t= ord $_m$ (a) = t. Así pues por el teorema 2.2 se infiere que s/t_1. (α)

Por otro lado, como $(a^u)^s = a^{us} \equiv 1 \bmod (m)$ se tiene que t/u s. De lo anterior, t_1 v/ u_1 vs y consecuentemente t_1 /u_1s. Por cuanto (t_1 u_1) = 1, aplicando el lema 2.3, se concluye que necesariamente t_1 / s. (β)

Finalmente de (α) y (β) se concluye que s= t_1 luego ord$_m$ (a^u) = $\frac{t}{v} = \frac{\text{ord m (a)}}{(t,u)}$ lo cual concluye la prueba.

Teorema 2.8

Si a,m son entero positivo relativamente primos y m tiene una raíz primitiva, entonces tiene en total $\varphi(\varphi\ (m))$ raíces primitivas no congruentes.

Prueba:

Sea r una raíz primitiva modulo m. Entonces los enteros r, r^2, ... $r^{\varphi(m)}$ constituyen un sistema residual reducido, por teorema 2.6, y como r^{φ}es una raíz primitiva módulo m si y solo si ($ord_m r$,u) = 1, por el teorema anterior y por cuanto solo hay $\varphi(\varphi(m))$ posibilidades para seleccionar a u, se concluye que hay exactamente $\varphi(\varphi(m))$ raíces primitivas módulo m.

Ejemplo:

Sea m=11.Se puede comprobar que 2 es una raíz primitiva módulo 11. En efecto, si calculamos $ord_{11}(2)$ tendremos que $\varphi(11) = 10$ y como

$2^1 = 2 \equiv 2 \bmod (11)$

$2^2 = 4 \equiv 4 \bmod (11)$

$2^3 = 8 \equiv 8 \bmod (11)$

$2^4 = 16 \equiv 5 \bmod (11)$

$2^5 = 32 \equiv 10 \bmod (11)$

$2^6 = 64 \equiv 9 \bmod (11)$

$2^7 = 128 \equiv 7 \bmod (11)$

$2^8 = 256 \equiv 3 \bmod (11)$

$2^9 = 512 \equiv 6 \bmod (11)$

$2^{10} = 1024 \equiv 1 \bmod (11)$

Así pues $\text{ord}_{11}(2) = 10$ como $\text{ord}_{11}(2) = \phi(11)$, se concluye que 2 es una raíz primitiva módulo 11.

Por otro lado, 6, 7 y 8 son también raíces primitivas módulo 11, como se puede calcular de manera análoga al cálculo para 2. Evidentemente, $\phi(\phi(11)) = \phi(10) = 4$, por lo cual de acuerdo al teorema 2.8, los enteros 2, 6, 7 y 8 forman un sistema residual reducido módulo 11.

Corolario 2.2:

Todo número primo tiene raíces primitivas.

Prueba:

Sea p un número primo, por la definición 2.2 existen $\varphi(p-1)$ enteros no congruentes módulo p cuyo orden es $p-1$. Como cada uno de estos es una raíz primitiva, se concluye que p tiene $\varphi(p-1)$ raíces primitivas.

En el desarrollo anterior se ha verificado que todo número primo tiene raíces primitivas. Ahora nos proponemos determinar todos los enteros positivos que tienen raíces primitivas. En primer lugar se mostrara que toda potencia de un primo impar posee raíces primitivas. Consideramos primero los cuadrados de números primos.

Teorema 2.9:

Sea p un primo impar, entonces p^k tiene una raíz primitiva para todo entero positivo k. Más aún, si r es una raíz primitiva módulo p^2, entonces r es una raíz primitiva módulo p^k para todo entero positivo k.

Prueba:

Del colorario 2.2 se sabe que p tiene una raíz primitiva r módulo p que es también una raíz primitiva módulo p^2, así pues $r^{p-1} \not\equiv 1 \ mod\ p^2$. (α)

Por inducción matemática, se verificará que para esta raíz primitiva r, la relación

$$rp^{k-2}(p-1) \not\equiv 1 \ mod\ (p^k). \qquad (\beta).$$

es válida para cualquier entero positivo k. Una vez establecida la relación (β), estaremos en condición de probar que r es también una raíz primitiva módulo p^k razonando del modo siguiente:

Si $n = ord_{pk}(r)$ entonces n divide a $\varphi(p^k) = p^{k-1}(p-1)$, que es una propiedad de la función de Euler.

Por otro lado, $r^n \equiv 1 \bmod (p^k)$. También sabemos que $r^n \equiv 1 \ mod\ (p)$. Por el Teorema 2.4 se sabe que $p - 1 = \varphi(p)/n$. Por cuanto $p - 1$ divide a n y a su vez n divide a

$p^{k-1}(p-1)$, se concluye que $n = p^t(p-1)$ donde t es un entero tal que $0 \leq t \leq k-1$.

Si $n = p^t(p-1)\ con\ t \leq k-2$, entonces $r^{p^{k-2}(p-1)} = (r^{p^t(p-1)})^{p^{k-2-t}} \equiv 1 \bmod (p^k)$, lo cual contradice la relación (β). De aquí, $ord_{p^k} = p^{k-1}(p-1) = \varphi(p^k)$, y en consecuencia r es una raíz primitiva módulo p^k.

Solo resta la verificación de (β) usando inducción matemática sobre k. El caso

k = 2 es consecuencia directa de (α).

Asumamos verdadera la afirmación (β) para todo $k \geq 2$. Entonces

$r^{p^{k-2}(p-1)} \not\equiv 1 \ mod\ (p^k)p$.

Como $(r,p) = 1$, se sabe que $(r,p^{k-1}) = 1$.

Consecuentemente, por el teorema de Euler se tiene que

$r^{p^{k-2}(p-1)} \equiv r^{\varphi(p^{k-1})} mod\ (p^{k-1}))$

Por lo anterior, existe un entero d tal que donde p no divide a d, pues por hipótesis $r^{p^{k-2}(p-1)} \not\equiv 1 \ mod\ (p^k)$. Tomando potencia p en ambos miembros de r se obtiene

$r^{p^{k-1}(p-1)} = (1 + dp^{k-1})^p$

$= 1 + p(dp^{k-1}) + \binom{p}{2}p^2(dp^{k-1})^2 + \ldots + (dp^{k-1})^p$

$\equiv 1 + dp^k (mod\ p^{k+1})$

Como p no divide a, d, se concluye que:

$r^{p^{k-1}(p-1)} \not\equiv 1 \ mod\ (p^{k+1})$.

Ejemplo: de los ejemplos anteriores se tiene que r = 3 es raíz primitiva de $\bar{7}$ y de $\bar{7}^2$. Así pues por el Teorema 2.9, $r = 3$ es también raíz primitiva *módulo* 7^k para todo entero positivo k.

Es el momento para discutir sobre la existencia de raíces primitivas de potencias de 2. Observemos primeramente que 2 y 2^2 tienen raíces primitivas, a saber 1 y 3 respectivamente. Para potencias de 2 mayores o iguales a tres, la situación es diferente a saber: "no hay raíces primitivas de potencias 2^k con k mayor que 2. Ya se vio que no hay raíces primitivas módulo 2^3.

Teorema 2.10:

Si a es un entero impar, y k un entero mayor o igual que 3, entonces

$$a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \ (mod\ 2^k)$$

Prueba:

Procederemos por inducción matemática sobre k. Si a es un entero impar entonces $a = 2b + 1$ donde b es un entero. De esto se infiere que:

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b\,(b+1) + 1.$$

Por cuanto b ó b+1 es par se observa que 4b (b+1) es divisible entre 8 y en consecuencia, $a^2 \equiv 1\ mod\ (8)$. Esta relación de congruencia resuelve el caso k=3.

En efecto, $a^{\varphi(2^3)/2} = a^{2^3-2^2/2} \equiv 1\ (mod\ 2^3)$

Para completar la inducción, asumimos que $a^{2^{k-2}} \equiv 1\ (mod\ 2^k)$, (Hip. Inductiva).

De esto último, existe un entero d tal que:

$$a^{2^{k-2}} = 1 + d2^k\,.$$

Elevando al cuadrado ambos miembros de esta igualdad se obtiene:

$$\left(a^{2^{k-2}}\right)^2 = 1 + d\,2^{k+1} + d^2\,2^{2k}$$

$$= 1 + d\,2^{k+1}\,(1 + d\,2^{k-1})$$

$$= 1\ mod\ (2^{k+1}),$$ lo cual complete la inducción.

Este teorema nos dice que ninguna potencia de 2, excepto 2 y 4, tiene raíz primitiva, puesto que cuando a es un entero impar, $ord_{2^k}a \neq \varphi\,(2^k)$, ya que

$$a^{2^k/2} \equiv 1\ (mod\ 2^k),$$

Hasta ahora se ha demostrado que todas las potencias de primos impares poseen raíces primitivas, en tanto que las únicas potencias de 2 que tiene raíces primitivas son 2 y 4. A continuación determinaremos aquellos enteros que no son potencias de primos, es decir enteros divisibles por dos o más primos y que poseen raíces primitivas. En efecto, se verificara que los únicos enteros que no son potencias de primos y que poseen raíz primitiva son el doble de una potencia de un primo impar.

Teorema 2.12:

Si n es un entero positivo que no es igual a una potencia de un primo o al doble de una potencia de primo, entonces n no tiene una raíz primitiva.

Prueba:

Sea n un entero positivo con factorización como producto se potencias de primos dados por:

$$n = p_1^{t_1}, p_2^{t_2} \dots p_m^{t_m}$$

Asumamos que n posee una raíz primitiva r. Esto significa que $(n, r) = 1$ y además $ord_n(r) = \varphi(n)$, por definición de raíz primitiva. Ahora bien, $(r, n) = 1$ implica que $(r, p^t) = 1$, donde p^t es una de las potencias que ocurren en la factorización de n. Por el teorema de Euler $r^{\varphi(p^t)} \equiv 1 \ (mod\ p^t)$

Consideremos el mínimo común múltiplo de $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \dots, \varphi(p_m^{t_m})$ y designémoslo por U.

Como $\varphi(p_i^{t_i})/U$ se puede afirmar que $r^U \equiv 1\ mod\ (p_i^{t_i})$, para cada i = 1,2,..., m.

En efecto, verificaremos que si r es una raíz primitiva módulo p^t, entonces si r es impar también es raíz primitiva módulo $2p^t$, en tanto que si r es par, $r + p^t$ es raíz primitiva módulo $2p^t$.

Prueba:

Si r es una raíz primitiva módulo p^t, entonces $r^{\varphi(p^t)} \equiv 1 \bmod (p^t)$, y ningún exponente positivo menor que $\varphi(p^t)$ satisface esta congruencia. Por la propiedad multiplicativa de la función de Euler, $\varphi(2p^t) = \varphi(2) \cdot \varphi(p^t)$, así que

$$r^{\varphi(2p^t)} \equiv 1 \ mod(p^t). \qquad (\alpha)$$

Si r es impar, entonces $r^{\varphi(2p^t)} \equiv 1 \ mod(2)$ ya que

$r = 2k + 1$, $(2k + 1)^{\varphi(2p^t)} \equiv 1 \ mod(2)$ (β).

De (α) y (β) se concluye que: $r^{\varphi(2p^t)} \equiv 1 mod(2p^t)$. Por cuanto ninguna potencia de r menor que $\varphi(2p^t)$ es congruente con 1 módulo $2p^t$, se concluye que r es una raíz primitiva módulo $2p^t$.

Por otro lado, si r es par, entonces $r + p^t$ es impar y por ello

$(r + p^t)^{\varphi(2p^t)} \equiv 1 \ mod \ (2)$ (*)

Como $r + p^t \equiv r \ mod \ (p^t)$, vemos que (**)

$(r + p^t)^{\varphi(2p^t)} = (r + p^t)^{\varphi(2)\cdot\varphi(p^t)} = (r + p^t)^{\varphi(p^t)} \equiv (r)^{\varphi(p^t)} mod(p^t) \equiv 1 \ mod(p^t$ (***)

Por lo tanto de (*) y (***) aplicando la propiedad multiplicativa de las congruencias, se llega a la conclusión $(r + p^t)^{\varphi(2p^t)} \equiv 1 \ mod(2p^t)$. (δ)

Por cuanto ninguna potencia menor de $r + p^t$ satisface (δ) se concluye que $r + p^t$ es una raíz primitiva módulo $2p^t$.

Ejemplo:

un entero impar, el teorema garantiza que $2 + 5^t$ es una raíz primitiva módulo $2 \cdot 5^t$, para todo $t > 0$. En especial, 27 es raíz primitiva de 50.

Resumiendo los resultados anteriores se puede describir los enteros positivos que tiene raíz primitiva de la siguiente manera:

Si n es un entero positivo mayor que 1, n tiene raíz primitiva si y solo si n es de la forma

$n = 2, 4, p^t$, o $2p^t$ siendo p un número primo impar y t un entero positivo.

2.3 El Lema de Hensel:

El lema de Hensel se originó en la teorías de los números p-adicos, pero tiene una formulación equivalente en la teoría de congruencias polinomiales, en esta investigación seguiremos esta última versión.

Sea $f(x)$ un polinomio con coeficientes enteros. Si $f(x_0) \equiv 0 \; mod(n)$, se dice que x_0 es una solución de la congruencia polinomial $f(x) \equiv 0$ mod(n). Estamos interesados en congruencias módulo un primo p. Estas congruencias tienen la forma:

$f(x) \equiv 0 \; mod(p^k)$ donde p es un primo y $k \geq 1$.

Puede demostrarse que todas las soluciones de $f(x) \equiv 0 \; mod(p^{k+1})$, (α)

pueden construirse a partir de las soluciones de $f(x) \equiv 0 \; mod(p^k)$ (β)

Específicamente, si x_1 es una solución de (α), podemos escribir $x_1 = x_0 + tpk$, donde x_0 es una solución de (β) y el entero t está por determinarse. Siguiendo la

literatura, se dice que la solución x_1 está por encima de x_0 ó también que x_0 se extiende a x_1. Presentamos a continuación el enunciado del lema de Hensel.

Teorema 2.14 (Lema de Hensel)

Sea $f(x)$ un polinomio con coeficientes enteros y $f'(x)$ es el polinomio derivado de $f(x)$,supongamos que p es un primo y

k $\geq$1. Sea r una solución de la congruencia polinomial $f(x) \equiv 0\ mod(p^k)$. Entonces solamente una de las siguientes proposiciones es verdadera.

i. Si $f'(r) \not\equiv 0\ mod(p^k)$ entonces r se extiende a una solución única r_1 de $f(x) \equiv 0\ mod(p^{k+1})$

   Esta solución está determinada por la regla $r_1 = r + tp^k$, donde

   $t = -\frac{r}{p}\left(f'(r)\right)^{-1}$.

Aquí se entiende que t es reducido $(mod\ p)$ si fuese necesario y que $\left(f'(r)\right)^{-1}$ es el inverso multiplicativo de $f'(r)$, en $\mathbb{Z}_p$.

ii. Si $f'(r) \equiv 0\ mod(p)$ y r es una solución de $f(x) \equiv 0\ mod(p^k)$, entonces r se extiende a $r_1 = r + tp^k$ para todos $0 \leq t \leq p-1$. Así pues r se extiende a p soluciones distintas a $f(x) \equiv 0\ mod(p^{k+1})$.

iii. Si $f'(r) \equiv 0\ mod(p)$ pero r no es una solución de $f(x) \equiv 0\ mod(p^k)$, entonces r, no se extiende a solución alguna de $f(x) \equiv 0\ mod(p^{k+1})$. Por lo tanto, si $f(x) \equiv 0\ mod(p^{k+1})$ tiene una solución r_1, ella no está encima de r.

Prueba:

Si r es una solución de $f(x) \equiv 0\ mod(p^k)$, entonces también es una solución de las congruencias $f(x) \equiv 0\ mod(p^{k-1})$. De aquí que dicha solución sea igual a $r + tp^{k-1}$, para algún t. La prueba termina una vez hayamos determinado el valor de t.

Por el Teorema de Taylor se sabe que:

$f(r + tp^k) = f(r) + f'(r)\, tp^{k-1} + \frac{f''(r)}{2!}(tp^k)^2 + \ldots + \frac{f^{(n)}(r)}{n!}(tp^k)^n$ donde $\frac{f^{(k)}(r)}{k!}$ es un entero para cada k = 1,2,..n.

Dado $k \geq 2$, se sigue que: $k+1 \leq m(k)$ y $p^{k+1} / p^{m(k)}$, para todo m tal que $2 \leq m \leq n$.

De esto último $f(r + tp^k) \equiv f(r) + f'(r)\, tp^k \ (mod\ p^k)$ $\quad (\alpha)$

Por cuanto $r + tp^k$ es una solución de $f(r + tp^k) \equiv 0\ mod(p^k)$, $\quad (\beta)$

por transitividad de (α) y (β) se concluye que : $f'(r)\, tp^k \equiv -f(r)\ mod(p^k)$.

Más aun dividiendo esta última congruencia p^k, ya que $f(r) \equiv 0\ mod(p^k)$, y arreglando términos se obtiene una congruencia lineal en t, a saber:

$$f'(r)t \equiv -f(r) / p^k\ (mod\ p). \quad (\delta)$$

Haciendo un análisis por disyunción de casos, de la congruencia anterior, se prueban las tres alternativas del lema.

1. Si $f'(r) \not\equiv 0\ mod(p)$, entonces f '(r) y p son relativamente primos, por lo cual (δ) tiene una solución única $t \equiv -\frac{f(r)}{p^{k-1}}\ \overline{f'(r)}$ (mod p) donde $\overline{f'(r)}$ es el inverso multiplicativo de f '(r) en $\mathbb{Z}_p$, lo cual establece el caso (i)

2. Si $f'(r) \equiv 0\ mod(p)$, entonces el máximo común divisor de $f'(r)$ y p es p.

   Luego si $p / \frac{f(r)}{p^{k-1}}$; lo cual es cierto si y sólo si $f(r) \equiv 0\ mod(p^k)$, entonces todos los valores de $t = 0,1,\ldots,p-1$ conducen a soluciones de (δ) .

   Esto es: $x = r + tp^{k-1}$ es una solución de (δ) para cada $t = 0,1,\ldots,p-1$.

   Esto prueba la condición (ii).

3. Finalmente, consideremos el caso para la cual $f'(r) \equiv 0\ mod(p)$ pero $p \nmid \frac{f(r)}{p^{k-1}}$.

   Bajo las condiciones, $(f'(r),p) = p\ y\ f(r) \not\equiv 0\ mod(p)$, por lo cual ningún valor de $r + tp^k$ es solución de (δ).

Corolario 2.3

Supongamos que r es una solución de la congruencia polinomial $f(x) \equiv 0\ mod(p)$, donde p es un entero primo. Si además $f'(r) \not\equiv 0\ mod(p)$, entonces hay una única raíz $r_k\ (mod\ p^k)$, tal que $k = 2,3,\ldots$ tal que $r_k = r_{k-1} - f(r_{k-1})\ \overline{f'(r)}$, donde $\overline{f'(r)}$ es el inverso de $f'(r)$ módulo p.

Prueba:

Aplicando las hipótesis y el lema de Hensel se observa que la solución r se extiende a una única solución r_2 (mod p^2) con $r_2 = r + tp$ y el valor de t está dado por $t = -\overline{f'(r)}\ \frac{f(r)}{p}$ de donde $r_2 = r - f(r)\ \overline{f'(r)}$. Por cuanto $r_2 \equiv r\ mod(p)$, se tiene que se deduce

$f'(r_2) \equiv f'(r) \not\equiv 0\ mod(p)$.

Aplicando el Lema de Hensel nuevamente, encontramos una solución r_3 módulo p^3, la cual está definida por $r_3 = r_2 - f(r_2)\,\overline{f'(r)}$.

Repitiendo este procedimiento, se ve que el corolario es válido para todo entero $k \geq 2$.

A continuación presentaremos un ejemplo que ilustra como se aplica el lema de Hensel.

Ejemplo:

Hallar las soluciones de la congruencia polinomial $x^3 + x^2 + 29 \equiv 0\ (mod\ 25)$

Solución:

Sea $f(x) = x^3 + x^2 + 29$. Por simple inspección se ve que las soluciones de $f(x) \equiv 0\ (mod\ 5)$ son $x \equiv 3\ mod\ (5)$. Por cuanto $f'(x) = 3x^2 + 2x$ y $f'(3) = 33$

$33 \equiv 3 \not\equiv 0 \bmod(5)$, el lema de Hensel nos dice que hay una solución única módulo 25 que es de la forma $3 + 5t$, donde $t \equiv -\overline{f'(3)}\left(\frac{f(3)}{5}\right) \bmod (5)$.

Aquí $\overline{f'(3)} = \bar{3} = 2$ ya que 2 es el inverso 3 mod (5). También debemos observar que $\frac{f(3)}{5} = \frac{65}{5} = 13$. En conclusión $t \equiv -2(3) \equiv 4\ (mod\ 5)$, Finalmente, $x \equiv 3 + 5(4) = 23$ es la única solución de $f(x) \equiv 0\ (mod\ 25)$.

Ejemplo:

Hallar las soluciones de la congruencia polinomial $x^2 + x + 7 \equiv 0\ mod\ (27)$.

Solución:

Sea $f(x) = x^2 + x + 7$: Las soluciones de $f(x) \equiv 0 \pmod 3$ son $x \equiv 1 \bmod (3)$.

f ′(x) = $2x + 1$, asi que y f ′(1) = 3 ≡ 0 (mod 3).

Más aún, por cuanto f (1) = 9 ≡ 0 (mod 9), se puede aplicar el caso (2) del lema de Hensel para concluir que 1 + 3t es una solución módulo 9 para todo entero t. Esto significa que las soluciones módulo 9 son x ≡ 1, 4 ó 7 (mod 9).

Por otro lado, por el caso (3) del lema de Hensel, ya que f (1) = 9 ≢ 0 (mod 27), no hay soluciones de f(x) ≡ 0 (mod 27) asociadas a x = 1 (mod 9).

Como f (4) = 27 ≡ 0 (mod 27), por el caso (2) del lema de Hensel, 4 + 9t es una solución mod 27 para todo entero t.

En consecuencia x ≡ 4, 13 ó 22 (mod 27) son soluciones del problema.

Finalmente, por el caso (3) del lema de Hensel, ya que f (7) = 63 ≢ 0 (mod 27), no hay soluciones de f(x) ≡ 0 (mod 27) asociadas a x ≡ 7 (mod 9).

Resumiendo, $x \equiv 4, 13$ ó $22\ (mod\ 27)$ son todas soluciones del problema

$f(x) \equiv 0\ (mod\ 27)$.

Ejemplo:

¿Cuáles son las soluciones de $f(x) = x^3 + x^2 + 2x + 26 \equiv 0$ (mod 343)?

Solución:

La soluciones de $f(x) \equiv 0\ (mod\ 7)$ son $x \equiv 2\ (mod\ 7)$. $f\,'(x) = 3x^2 + 2x + 2$ implica que

$f'(2) = 18 \not\equiv 0 \pmod 7$, se puede aplicar el corolario del lema de Hensel para hallar soluciones $mod\ 7^k$ para $k = 2,3,\ldots$

Observemos que $\overline{f'(2)} = \overline{18} = 2\ (mod\ 7)$.

Para encontrar $r_2 = 2 - f(2)\,\overline{f'(2)}$

$= 2 - 42\,(2)$

$= = 82$

$\equiv 16\ mod\ (7^2)$

Y $r_3 = 16 - f(16)\,\overline{f'(16)}$

$= 16 - 4410\,(2)$

$= -8804$

$\equiv 114 \pmod{343}$

En resumen, las soluciones de $f(x) \equiv 0\ (mod\ 343) son$ todos los enteros x tales que $x \equiv 114\ (mod\ 343)$.

III. CONSTRUCCIÓN DE RAÍCES PRIMITIVAS DE POTENCIAS DE PRIMOS

III.CONSTRUCCIÓN DE RAÍCES PRIMITIVAS DE POTENCIAS DE PRIMOS

En este capítulo se presentan cuatro resultados que constituyen la parte medular de la tesis.

El primero de ellos se describe una condición suficiente para que una potencia de una raíz primitiva sea también raíz primitiva.

El segundo resultado nos permite encontrar raíces primitivas para el cuadrado de un número primo impar p en términos de las raíces primitivas del mismo p.

El tercer resultado es una especie de generalización del segundo por cuanto permite construir las raíces primitivas del cuadrado de un número primo p mediante un algoritmo que resalta un valor excepcional del parámetro que define el algoritmo en cuyo caso no se obtiene una raíz primitiva para p^2.

El último resultado del capítulo caracteriza todas las raíces primitivas de la potencia p^{k+1} en términos de las raíces primitivas de p^k, siendo p un primo impar y k un entero positivo mayor igual que dos.

Teorema 3.1 Sea r una raíz primitiva módulo m, m > 1. Entonces r^u es una raíz primitiva módulo m si y solo si $(u,\varphi(m)) = 1$

Prueba:

Por el teorema (2.7) se sabe que $\text{ord}_m(r^u) = \frac{ord_m(r)}{(ord_m(r),u)} = \frac{\phi(m)}{(\phi(m),u)}$ (α)

Ya que r es por hipótesis una raíz primitiva módulo m. Ahora bien, si r^u es una raíz primitiva entonces $ord_m(r^u) = \phi(m)$, luego de la igualdad anterior, $ord_m(r^u) = \frac{\phi(m)}{(\phi(m),u)}$, de donde $\phi(m) = \frac{\phi(m)}{(\phi(m),u)}$, lo cual implica que $(\phi(m), u) = 1$

Recíprocamente, si $(\phi(m), u) = 1$ entonces nuevamente de la igualdad α) deduce que $ord_m(r^u) = \phi(m)$, lo cual por definición significa que r^u es una raíz primitiva módulo m.

Ejemplo:

3 es una raíz primitiva de 7, ya que $\varphi(7) = 6 = ord_7(3)$. Aplicando el teorema 2.8, como (5,6) =1 se debe verificar que 3^5 es raíz primitiva de 7. En efecto, $3^5 = 243 \equiv 5 \mod (7)$ y como 5 es raíz primitiva de 7, entonces 3^5 también lo es.

Análogamente, como ya hemos visto que 5 es es raíz primitiva de 7. Aplicando el teorema 2.8, 5^5 debe ser también raíz primitiva de módulo 7, ya que (5,6) =1.

Teorema 3.2

Si p es un número primo impar con raíz primitiva r, entonces o bien r ó r + p es una raíz primitiva módulo p^2.

Prueba:

Como r es por hipótesis una raíz primitiva módulo p, entonces de acuerdo a la definición $ord_p(r) = \varphi(p) = p - 1$.

Sea $n = ord_{p^2}(r)$, de modo que: $r^n \equiv 1 \ mod(p^2)$ por definición de orden. Tenemos que

$r^n \equiv 1\ mod(p)$. Por el teorema 2.7, $p - 1 = ord_p(r)$ divide a n. Por otro lado, por el corolario 2.3 sabemos que n divide a $\varphi(p^2) = p(p-1)$. Como $n \,/\, p(p-1)$ y $(p-1)/n$; ó bien $n = p-1$ ó $n = p(p-1)$.

Si $n = p(p-1)$ entonces r es una raíz primitiva módulo p^2, ya que $ord_p{}^2(r) = \varphi(p^2)$ por definición de raíz primitiva. Por otro lado, si $n = p-1$ tendríamos que $r^{p-1} \equiv 1\ mod(p^2)$.

Sea $S = r + p$. Entonces como $S \equiv r\ mod(p)$, S es también una raíz primitiva módulo p.

De lo anterior, $ord_p{}^2(S)$ es $p-1$ ó $p(p-1)$.

Verificamos que $ord_p{}^2(S)$ no puede ser p-1. En efecto, por el teorema del binomio tenemos que:

$$S^{p-1} = (r+p)^{p-1}$$

$$= \sum_{i=0}^{p-1} \binom{p-1}{i} r^i p^{(p-1)-i}$$

$$\equiv (r^{p-1} + (p-1)\, r^{p-2} \cdot p)\ mod\ (p^2)$$

$$\equiv (1 + (p-1)\, r^{p-2} \cdot p)\ mod\ (p^2)$$

$$\equiv (1 + p^2\, r^{p-2} - pr^{p-2})\ mod\ (p^2)$$

$$\equiv (1 - pr^{p-2})\ mod\ (p^2)$$

Luego $S^{p-1} - 1 \equiv -pr^{p-2}\ mod\ (p^2)$, de donde se concluye que $S^{p-1} \not\equiv 1\ mod\ (p^2)$. Para ver esto último, notemos que si fuese cierto que $S^{p-1} \equiv 1 mod\ (p^2)$ entonces $p\, r^{p-2} \equiv 0 \bmod (p^2)$. De esto se concluirá que $r^{p-2} \equiv 0 \bmod (p^2)$, lo cual es imposible ya que p no divide a r, pues r es raíz primitiva de p. En conclusión

En el siguiente cuadro presentaremos algunas situaciones que pueden ocurrir con relación al resultado del Teorema 3.2

r es una raíz primitiva módulo p y se cumple que r es raíz primitiva módulo p^2 pero r + p no es raíz primitiva módulo p^2.

Sea r = 2, p = 5. Ya hemos visto que el orden de 2 módulo 5 es 4 que es precisamente el valor $\varphi(5)$. Así pues 2 es una raíz primitiva módulo 5. Y $orden_{25}(2) = 20 = \varphi(5^2)$ pero 2 + 5 no es raíz primitiva de 25 pues $orden_{25}(7) = 4 \neq \varphi(5^2)$

r si, r + p no	p = 5 , r = 2
r si, r + p si	p =11 , r = 2
r no, r + p si	p = 487 , r = 10

Observación: m es una raíz primitiva módulo m (cuando m posee raíces primitivas) Si $Orden_m(n) \equiv \varphi(m)$

Ejemplo:

Sea p = 7, ya hemos verificado r = 3 es una raíz primitiva mod 7. En efecto tal como se muestran en los cálculos siguientes

$Ord_7 3 = \varphi(7) = 6$

$3^1 = 3 \equiv 3 \ mod \ 7$

$3^2 = 9 \equiv 2 \ mod \ 7$

$3^3 = 27 \equiv 6 \ mod\ 7$

$3^4 = 81 \equiv 4 \ mod\ 7$

$3^5 = 243 \equiv 5 \ mod\ 7$

$3^6 = 729 \equiv 1 \ mod\ 7$

$r_1 = 3$ es raíz primitiva mod 49 ó $r_2 = 10 = 3+7$ es raíz primitiva mod 49.

Observación:

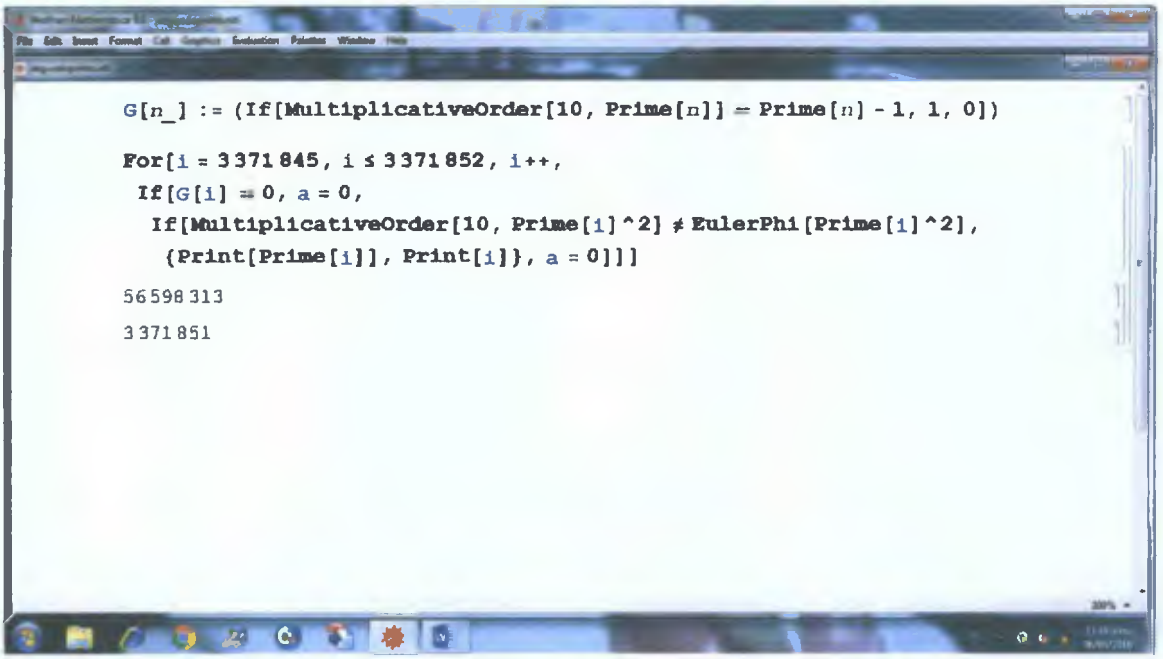
Notemos que es extremadamente raro que la congruencia $r^{p-1} \equiv 1 \ mod\ (p^2)$ no sea verdadera cuando r es una raíz primitiva módulo p. Consecuentemente es muy inusual que una raíz primitiva r módulo el número primo p no sea una raíz primitiva módulo p^2. El número primo más pequeño p para el cual hay una raíz primitiva que no sea una raíz primitiva módulo p^2 es p = 487.

p = 487, 10 es raíz primitiva *módulo* 487. Esto es $ord_{487}(10) = \varphi(487) = 486$

En efecto, $p - 1 = 486 = 2 \cdot 243 = 2 \cdot 3^5$ tiene 12 divisores,

1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 243 y 486. Los valores de $10^n \ mod(487)$ se muestran en la tabla a continuación

N	$10^n \ mod(487)$	N	$10^n \ mod(487)$
1	10	27	446
2	100	54	220
3	26	81	233
6	189	162	232
9	44	243	486
18	475	486	1



Con la implementación de este código encontramos que el próximo primo p con la propiedad que 10 es raíz primitiva módulo p pero no módulo p^2 es 56598313.

Observación:

1. No hay otro primo con esta propiedad entre los primeros $5x10^6$ primos.
2. El próximo primo debe ser mayor que $8x10^7$.

Teorema 3.3

Si p es un número primo y r es una raíz primitiva de p, entonces $r + tp$ es una raíz primitivas de p^2 para todos los valores de t tales que $0 \leq t \leq p\text{-}1$ excepto uno. Este valor excepcional de t está dado por la fórmula $t = \frac{1-r^{p-1}}{p}\left((p-1)r^{p-2}\right)^{-1}$, donde t es

reducido $mod(p)$ si es necesario y $\left((p-1)r^{p-2}\right)^{-1}$ denota al inverso multiplicativo de $(p-1)r^{p-2}\ mod(p)$.

Prueba:

Mostremos que si r es una raíz primitiva $mod(p)$ entonces $r + tp$ es una raíz primitivas de p^2 para exactamente p-1 valores de t $mod(p)$.

Denotemos con h el orden $r + tp \ mod\ (p^2)$. Así pues h puede depender de t. Por lo tanto, $(r + tp)^h \equiv 1\ mod(p^2)$. Así púes, $(r + tp)^h$ -1 es un múltiplo de p^2. Como consecuencia inmediata resulta que $(r + tp)^h$ -1 es también múltiplo de p. Esto último se traduce en términos de congruencia en la forma

$(r + tp)^h \equiv 1\ mod(p)$. Sin embargo, el desarrollo del binomio $(r + tp)^h$ contiene $h + 1$ términos cada uno de los cuales contiene el factor p excepto el primero, esto es r^h. De esto se desprende que si $(r + tp)^h \equiv 1\ mod(p)$ entonces $(r)^h \equiv 1\ mod(p)$. En conclusión, el orden de $r\ mod(p)$ tiene que ser un divisor de h. Pero dicho orden es precisamente

φ (p) = p – 1 ya que g es una raíz primitiva módulo p. Así pues p – 1/ h. Por otro lado, por el teorema 2.7 se sabe que h/ φ (p^2) = $p(p-1)$. En conjunto, estas dos relaciones de divisibilidad nos conducen a la conclusión $h = p - 1$ ó $h = p\ (p-1)$. En la segunda opción

$r + tp$ es una raíz primitiva $mod\ (p^2)$ y en el primero no lo es. Verificaremos que cuando

$r + tp$ es una raíz primitiva, esto ocurre para solamente uno de los posibles valores de t. Sea $f(x) = x^{p-1} - 1$, en el caso que nos ocupa, $r + tp$ es una solución de la congruencia $f(x) \equiv 0\ mod(p^2)$ que está por arriba de $r\ mod(p)$.

Como $f'(r) = (p-1)r^{p-2} \not\equiv 0\ mod(p)$, por el Lema de Hensel se sabe que $r\ mod(p)$ se extiende a una única solución $(r + tp^2)\ mod(p^2)$. Para todos los otros valores de $t\ mod(p)$, los números $r + tp$ son raíces primitivas $mod(p^2)$.

Como cada una de las $\varphi(p-1)$ raíces primitivas $mod(p)$ da lugar a exactamente $p-1$ raíces primitivas de p^2, hemos mostrado que existen al menos $(p-1)\,\varphi(p-1)$ raíces primitivas $mod(p^2)$

Para mostrar que no hay otras raíces primitivas $mod(p^2)$, razonamos como sigue:

sea r una raíces primitivas de p^2, de modo que los números $r, r^2, \ldots r^{p(p-1)}$ forman un sistema residual reducido módulo p^2. Por el teorema 3.3, r^k es una raíz primitiva si y solo sí

$(k, p(p-1)) = 1$. De acuerdo a la definición de la función φ de Euler, existen precisamente $\varphi(p(p-1))$ valores posibles para k entre los enteros 1,2, ... $p(p-1)$. Como $(p, p-1) = 1$ se deduce del carácter multiplicativo de φ que

$$\varphi(p(p-1)) = \varphi(p)\,\varphi(p-1)) = (p-1)\,\varphi(p-1).$$

A continuación construiremos las raíces primitivas de $3^2 = 9$. Fácilmente se verifica que 2 es la única raíz primitiva del primo 3, así pues por el Teorema 3.1 se llega a la

conclusión que 2 + 3t es una raíz primitiva de 3^2para todo valor de t tal que $0 \leq t \leq 2$, excepto para

$$t = \frac{1-2^{3-1}}{3}\left((3-1)2^{3-2}\right)^{-1} = \frac{-3}{3}(4)^{-1} = -1 \cdot 1 = -1 \equiv 2(mod3)$$

Por lo tanto, los números $2 + 3\cdot0 = 2$ y $2 + 3\cdot1 = 5$ son raíces primitivas de 3^2 y $2 + 3\cdot2 = 8$ no es raíz primitiva. Más aún, como 2 es la única raíz primitiva de 3 se concluye que 2 y 5 son las raíces primitivas de 3^2.

Como segundo ejemplo, calculamos las raíces primitivas de $5^2 = 25$. Directamente se puede verificar que 2 y 3 son las únicas raíces primitivas de 5. En efecto,

$ord_5(2) = ord_5(3) = \varphi(5) = 4$ y además $\varphi(\varphi(5)) = \varphi(4) = 2$, luego 5 solamente tiene 2 raíces primitivas, a saber 2 y 3. Aplicando el teorema 3.3 se concluye que los números $2 + 5t_1$; $0 \leq t_1; \leq 4$ y $3 + 5t_2$; $0 \leq t_2 \leq 4$ son raíces primitivas de $5^2 = 25$ para todos los valores de t_1 y t_2 / $0 \leq t_1, t_2 \leq 4$ excepto para:

$$t_1 = \frac{1-2^{5-1}}{5}\left((5-1)2^{5-2}\right)^{-1} = \frac{-15}{5}(32)^{-1} = -3 \cdot 2^{-1} = (-3)(3) = -9$$

$$\equiv 1(mod5)$$

$$t_2 = \frac{1-3^{5-1}}{5}\left((5-1)3^{5-2}\right)^{-1} = \frac{-80}{5}(4(27)^{-1} = -16 \cdot 108^{-1} = (-16)(3)^{-1}$$

$$= (-16)(2) - 32 \equiv 1(mod5)$$

Los cálculos que se muestran a continuación producen raíces primitivas de $5^2 = 25$

$2 + (0)(5) = 2$ $\qquad$ $3 + (0)(5) = 3$

$2 + (2)(5) = 12$ $3 + (1)(5) = 8$

$2 + (3)(5) = 17$ $3 + (2)(5) = 13$

$2 + (4)(5) = 22$ $3 + (4)(5) = 23$

Nuevamente, como 2 y 3 son las únicas raíces primitivas de 5, entonces por el teorema 3.3 los resultados anteriores constituyen todas las raíces primitivas de 5^2.

Como tercer ejemplo, calculamos las raíces primitivas de $\bar{7}^2 = 49$, aplicando el algoritmo $r = r_0 + 7t$, con $0 \leq t \leq 6$, donde r_0 es una raíz primitiva de 7.

Se puede verificar que 3 y 5 son raíces primitivas de 7. Apliquemos el algoritmo a

$r_0 = 3,\ r_0 = 5$. En el primer caso $r_0 = 3$, tendremos que $r = 3 + 7t$, con $0 \leq t \leq 6$ son raíces primitivas de 49, excepto para el valor de

$$t_1 = \frac{1 - 3^{7-1}}{7}\left((7-1)3^{7-2}\right)^{-1} = \frac{6(1-729)}{7}(243)^{-1} = \frac{-6(728)(3)}{7} = -1872$$

$$\equiv -3 \equiv 4 mod(7)$$

Luego para todo $0 \leq t \leq 6$ excepto $t = 4$, la expresión $r = 3 + 7t$ produce raíces primitivas de 49 que es 7^2.

Para $r_0 = 5$, tendremos que la expresión $r = 5 + 7t$ produce raíces primitivas para 49 excepto para

$$t_2 = \frac{1 - 5^{7-1}}{7}\left((7-1)5^{7-2}\right)^{-1} = \frac{6(1-15625)}{7}(3125)^{-1} = \frac{-6(15624)(5)}{7}$$

$$\equiv 0\, mod(7)$$

En conclusión el valor excepcional ocurre cuando $t = 0$, por lo tanto $r = 5$ es raíz primitiva de 7 pero no de 49.

El teorema principal de la investigación nos muestra como extender la construcción anterior para hallar las raíces primitivas de potencias arbitrarias de números primos impares.

Teorema 3.4:

Si p es un primo impar, y k ≥ 2 y g es una raíz primitiva de p^k, entonces $r + tp^k$ es una raíz primitiva de p^{k+1} para todo valor de t tal que $0 \leq t \leq p - 1$. Más aún todas las raíces primitivas de p^{k+1} se construyen de esta manera.

Prueba:

Primero se prueba que para cualquier valor de t, $0 \leq t \leq p - 1$, ó $r \not\equiv tp^k$ es una raíz primitiva de p^{k+1} o bien $ord_{p^{k+1}}(r + tp^k) = \varphi(p^k)$.

Sea $h = ord_{p^{k+1}}(r + tp^k)$ entonces $(r + tp^k)^h \equiv 1 mod (p^{k+1})$ y así también

$(r + tp^k)^h \equiv 1 \bmod (p^k)$

Ahora bien $r \equiv (r + tp^k) \ mod \ p^k$ luego $r^h \equiv (r + tp^k)^h \equiv 1 \ mod \ (p^k)$. Esta última congruencia significa que h es un múltiplo del $ord_{p^k}(r)$, el cual es $\varphi(p^k)$ por cuanto r es una raíz primitiva módulo p^k. Así pues, se puede escribir $h = y \ \varphi(p^k)$ para algún entero y positivo. Por otro lado, h se definió como el $ord_{p^{k+1}}(r + tp^k)$ que es precisamente $\varphi(p^{k+1}) = p\,\varphi(p^k)$. Por lo tanto

p $\varphi(p^k)$ = (x)(h), para algún entero positivo x sustituyendo las ecuaciones anteriores obtenemos: $p\ \varphi(p^k) = (x)(h) = (x)(y)\ \varphi(p^k)$, la cual implica que $xy = p$.

Como p es primo, y es positivo se concluye que o bien $y = p$ ó $y = 1$.

De acuerdo a la igualdad h = y $\varphi(p^k)$, esta última información acerca de y nos dá:

h = p $\varphi(p^k) = \varphi(p^{k+1})$ ó h = $\varphi(p^k)$.

En el primer caso, $r + t\ p^k$ es una raíz primitiva de p^{k+1} y en el segundo caso tendremos que $ord_{p^{k+1}}\ (r + tp^k)$ es $\varphi(p^k)$.

De lo anterior se concluye que para dar una demostración del teorema 3.4, basta con mostrar que $ord_{p^{k+1}}\ (r + tp^k) \neq \varphi(p^k)$, para todos los valores de $0 \leq t \leq p - 1$. Por reducción al absurdo, supongamos que existe algún valor de t comprendido entre cero y p – 1 tal que $ord_{p^{k+1}}\ (r + tp^k) = \varphi(p^k)$ entonces $(r + tp^k)^{\varphi(p^k)} \equiv 1\ mod\ (p^{k+1})$.

Así pues,$(r + tp^k)$ es una solución de la congruencia f(x) ≡ 0mod (p^{k+1}) donde $f(x) = x^{\varphi(p^k)} - 1$.

Como g es una raíz primitiva de p^k, g es una solución de f(x) ≡ 0 mod (p^k) y por tanto r se extiende a $r + tp^k$.

Ahora $f' = \varphi(p^k)\ (x)^{\varphi(p^k)-1}$, cuyo valor en $x = r$ es:

$$f' = \varphi(p^k)\ r^{\varphi(p^k)-1} = (p^k - p^{k-1}) = r^{\varphi(p^k)-1} = p(p^{k-1} - p^{k-2}) = r^{\varphi(p^k)-1} \equiv 0\ mod\ (p).$$

Como las relaciones anteriores son falsas si $k = 1$, es necesario suponer que $k \geq 2$.

Finalmente, como r es una raíz primitiva de p^2, por el teorema 3.3 se concluye que r es una raíz primitiva de p^{k+1}. De lo anterior $r^{\varphi(p^k)} \not\equiv 1 \ mod(p^{k+1})$ ya que

$\varphi(p^k) < \varphi(p^{k+1}) = ord_{p^{k+1}}(r)$, por lo cual r no es solución de $f(x) \equiv 0 \ mod\ (p^{k+1})$, la cual es una contradicción por consiguiente,

$ord_{p^{k+1}}(r + t\,p^k) \neq \varphi(p^k)$ para todo t tal que $0 \leq t \leq p-1$, de donde $r + t\,p^k$ es una raíz primitiva de p^{k+1} para todo t tal que $0 \leq t \leq p-1$. Solo falta verificar que todas las raíces primitivas de p^{k+1} se construya de manera descrita anteriormente. En efecto, al variar t desde 0 hasta $p-1$, tp^k recorre todos los valores desde $0, p^k$...hasta $(p-1)p^k$, todos múltiplos de de p^k. Como estos son diferentes módulo p^{k+1}, se sigue que los números $r + t\,p^k$ son distintos $mod\ (p^{k+1})$,para todo t en el intervalo $[0, p-1]$. Más aún, si r_1 y r_2 son raíces primitivas de p^k y $0 \leq t_1, t_2 \leq p-1$, entonces

$r_1 + t_1\,p^k \equiv r_2 + t_2\,p^k\ mod\ (p^{k+1})$,lo cual implica que $r_1 + t_1\,p^k \equiv r_2 + t_2\,p^k\ mod\ (p^k)$ y así

$r_1 - r_2 \equiv (t_1 - t_2)\,p^k \bmod (p^k) \equiv 0 \bmod (p^k)$ de donde $r_1 \equiv r_2\ 0 \bmod (p^k)$.

Al variar g entre todas las $\varphi(\varphi(p^k))$ raíces primitivas de p^k y t recorre libremente los valores $0,1,\ldots,p-1$, se contará con el numero $p \cdot \varphi(\varphi(p^k))$ de raíces primitivas p^{k+1} tal como se puede verificar, la igualdad $p \cdot \varphi\left(\varphi(p^k)\right) = \cdot\ \varphi\left(\varphi(p^{k+1})\right)$ es verdadera y nos muestra que se han construido todas las raíces primitivas p^{k+1} exactamente una sola vez.

Ejemplo:

Construcción de la raíces primitivas de $3^3 = 27$ a partir de $3^2 = 9$. Los cálculos anteriores nos dieron como resultado que:

$2 + (0)(3^2) = 2$ $\qquad$ $5 + (0)(3^2) = 5$

$2 + (1)(3^2) \equiv 11$ $\qquad$ $5 + (1)(3^2) \equiv 14$

$2 + (2)(3^2) = 20$ $\qquad$ $5 + (2)(3^2) = 23$

Son todas las raíces primitivas de 3^3.

Como 2 y 5 son las únicas raíces primitivas de 3^2 los resultados obtenidos agotan la totalidad de las raíces primitivas de 3^3. Ahora que sabemos que 2, 5, 11, 14, 20 y 23 son las raíces primitivas de 3^3 podemos calcular todas las raíces primitivas de 3^4 aplicando nuevamente el teorema 2.9 obteniendo los resultados que se presentan a continuación

$\bar{2} + \bar{3}^3 \cdot \bar{0} = \bar{2}$ $\qquad$ $\bar{2} + \bar{3}^3 \cdot 1 = \bar{29}$ $\qquad$ $\bar{2} + \bar{3}^3 \cdot \bar{2} = \bar{56}$

$5 + 3^3 \cdot 0 = 5$ $\qquad$ $5 + 3^3 \cdot 1 = 32$ $\qquad$ $5 + 3^3 \cdot 2 = 59$

$11 + 3^3 \cdot 0 \equiv 11$ $\qquad$ $11 + 3^3 \cdot 1 \equiv 38$ $\qquad$ $11 + 3^3 \cdot 2 \equiv 65$

$14 + 3^3 \cdot 0 = 14$ $\qquad$ $14 + 3^3 \cdot 1 = 41$ $\qquad$ $14 + 3^3 \cdot 2 = 68$

$20 + 3^3 \cdot 0 = 20$ $\qquad$ $20 + 3^3 \cdot 1 = 47$ $\qquad$ $20 + 3^3 \cdot 2 = 74$

$23 + 3^3 \cdot 0 = 23$ $\qquad$ $23 + 3^3 \cdot 1 = 50$ $\qquad$ $23 + 3^3 \cdot 2 = 77$

- Ampliar el estudio hacia las aplicaciones de la noción de raíces primitivas a la criptografía.
- Investigar sobre las raíces primitivas de Fibonacci.

Rosen , K. (1999). *Elementary Number They And Its Applications.* Massachusetts: Addison-Wesley.

Strayer, J. (2002). *Elementary Number Theory.* Waveland Press Inc.

Varona, J. L. (2014). *Recorridos por la Teoría de Números.* E-lectolibris.

Watkins, J. (2014). *Number Theory. A Historical Approach.* Princeton University Press.

Vornicu, V. (2005). Exactly 2000 prime divisor. *www.artofproblemsolving.com*, AoPS topic #57607.

Wofram, S. (1987). *Wolfram Computations Meers Knowledge*. Recuperado el 19 de Julio de 2014, de https://www.wolfram.com/mathematica/